A Game Theory Based Reputation Mechanism to Incentivize Cooperation in Wireless Ad Hoc Networks[☆]

Juan José Jaramillo[*], R. Srikant

Coordinated Science Laboratory and Dept. of Electrical and Computer Engineering, University of Illinois, Urbana-Champaign, IL 61820, United States

Abstract

In wireless ad hoc networks one way to incentivize nodes to forward other nodes' packets is through the use of reputation mechanisms, where cooperation is induced by the threat of partial or total network disconnection if a node acts selfishly. The problem is that packet collisions and interference may make cooperative nodes appear selfish sometimes, generating unnecessary and unwanted punishments. With the use of a simple network model we first study the performance of some proposed reputation strategies and then present a new mechanism called DARWIN (Distributed and Adaptive Reputation mechanism for WIreless ad hoc Networks), where we try to avoid retaliation situations after a node is falsely perceived as selfish to help restore cooperation quickly. Using game theory, we prove that our mechanism is robust to imperfect measurements, is collusion-resistant and can achieve full cooperation among nodes. Simulations are presented to complement our theoretical analysis and evaluate the performance of our algorithm compared to other proposed reputation strategies.

Key words: ad hoc networks, wireless networks, reputation mechanisms, incentive schemes, cooperation enforcement

[☆]This paper is a revised version of an earlier paper that appeared in Mobicom 2007 [1].

[*]Corresponding author

Email addresses: jjjarami@illinois.edu (Juan José Jaramillo), rsrikant@illinois.edu (R. Srikant)

1. Introduction

Wireless ad hoc networks consist of a set of self-configuring nodes that do not rely on any infrastructure to communicate among each other. To achieve this goal, a source communicates with a distant destination through intermediate nodes that act as relays. It is usually assumed that in such networks, nodes are willing to cooperate forwarding packets, but this assumption is not necessarily true in the case where all nodes are not under the control of a single authority. In these cases, there can be selfish nodes that want to maximize their own welfare without regard to social welfare, where we define a node's welfare as the benefit of its actions minus the cost of its actions. In such scenarios, cooperation cannot be taken for granted and therefore, it is necessary to develop mechanisms that allow cooperation to emerge even in the presence of selfish users.

Incentive mechanisms can be broadly divided in two categories: credit-exchange systems and reputation-based systems. In credit-exchange systems [2, 3, 4, 5, 6, 7, 8], cooperation is induced by means of payments received every time a node acts as a relay and forwards a packet, and such credit can later be used by these nodes to encourage others to cooperate. To guarantee that nodes do not counterfeit payments, some strategies rely on the use of tamper-proof hardware to store credit and guarantee the check and balances, but this strategy may hinder their ability to find wide-spread acceptance; other strategies rely on the presence of an off-line central trusted authority which may be hard to guarantee in some scenarios. In reputation-based strategies [9, 10, 11, 12, 13, 14, 15, 16, 17], a node's behavior is measured by other nodes in the network. Selfish behavior is then discouraged by the threat of partial or total network disconnection. The problem is that due to interference and collisions it is not always possible to perfectly estimate how a node behaves, so sometimes cooperative nodes are perceived as being selfish and punished accordingly; such scenarios can lead to retaliation situations that may potentially decrease the throughput of cooperative nodes.

The contributions of this paper are twofold: first, we use a simple game-theoretic network model to study the robustness of some previously proposed reputation-based strategies. We show that some strategies are not self-enforcing, meaning that there is an incentive to deviate from the expected behavior, while others punish selfish behavior at the expense of the throughput of cooperative nodes, potentially leading to complete network disconnection due to retaliation. Second, we propose a new strategy called

Table 1: Payoff Matrix of the Prisoners' Dilemma Game

		Player 2			
		Cooperate		Defect	
Player 1	Cooperate	1	1	−1	2
	Defect	2	− 1	0	0

DARWIN (Distributed and Adaptive Reputation mechanism for WIreless ad hoc Networks) that effectively detects and punishes selfish behavior. We derive conditions under which no node can gain from deviating from our strategy, prove that full cooperation can emerge among nodes, and that our scheme is collusion resistant.

Simulations are also presented to complement the theoretical contributions. Our results show that the throughput achieved with DARWIN is better than any of the other strategies studied, and that DARWIN can be implemented with low overhead.

The rest of the paper is organized as follows. Section 2 introduces some concepts from game theory that are used in this paper. In Section 3 we define the network model which will be used in Section 4 to analyze some of the previously proposed strategies. We introduce our strategy in Section 5, analyze the conditions under which cooperation can emerge, study its performance, and show that it is relatively insensitive to parameter choices. The impact of collusion among nodes is also studied there. Section 6 presents the results of a simulation-based study of DARWIN and how it compares to other reputation-based strategies. Section 7 presents an overview of related work. Finally, Section 8 presents the conclusions.

2. Basic Game Theory Concepts

Here we introduce the concepts from game theory [18] that are used in this paper. As an illustration, we use a well-known game between two players known as *The Prisoners' Dilemma*. Both players have two possible *pure strategies*, Cooperate (C) or Defect (D), and the payoffs they receive for their actions are given in Table 1. Then player i's *strategy space* S_i is defined to be the set of pure strategies available to it. In this case $S_i = \{C, D\}$ for

$i = \{1, 2\}$. A *strategy profile* is defined to be an element of the product-space of strategy spaces of each player. An example is for player 1 to play D and player 2 to play C.

Definition 1. *A* Nash equilibrium *is a strategy profile having the property that no player can benefit by unilaterally deviating from its strategy.*

Such a strategy profile is considered to be *self enforcing*. In this example, the Nash equilibrium would be the strategy profile $s = (D, D)$. Assume now that this game is repeated infinitely many times, and for each k, the outcomes of the $k-1$ preceding plays are observed before the k-th stage begins. In this case, the total payoff of the game for player i is the discounted sum of the stage payoffs. Denoting the stage payoffs by $u_i^{(k)}$, the total payoff is given by

$$U_i = \sum_{k=0}^{\infty} w^k u_i^{(k)} \ ,$$

where $w \in (0, 1)$ is the *discount factor*. The infinitely repeated game can also be interpreted as a repeated game that ends after a random number of repetitions. Under this interpretation, the length of the game is a geometric random variable with mean $1/(1-w)$.

In this game a player's strategy specifies the action it will take at each stage, for each possible history of play through previous stages. In our example a strategy for player 1 could be to cooperate until player 2 defects, and then defect forever. Since both players know the previous history, we can view the game starting at stage k with a given history h^k as a new game; this is called a *subgame* of the original game.

Definition 2. *For a given set of strategies that are in Nash equilibrium, history h^k is* on the equilibrium path *if it can be reached with positive probability if the game is played according to the equilibrium strategies, and is* off the equilibrium path *otherwise.*

Definition 3. *A Nash equilibrium is* subgame perfect *if the player's strategies constitute a Nash equilibrium in every subgame.*

Subgame perfection is a stronger concept that eliminates *noncredible* equilibria, since it analyzes the case when a game is on or off the equilibrium path. This will later help us analyze whether a given reputation scheme is robust enough to handle the case when due to inaccurate measurements nodes appear to be out of their predicted behavior.

Definition 4. *A game is* continuous at infinity *if for each player i the payoff U_i satisfies:*

$$\sup_{h,\tilde{h}\ s.t.\ h^k=\tilde{h}^k} \left| U_i(h) - U_i(\tilde{h}) \right| \to 0 \ as\ k \to \infty$$

Under this definition, events in the distant future are relatively unimportant. This holds true if the total payoff of the game is the discounted sum of the per-period payoffs $u_i^{(k)}$, and the per-period payoffs are uniformly bounded. In our example this holds true since $u_i^{(k)} \leq 2$ for all k.

Lemma 1 (One-Stage Deviation Principle). *In an infinite-horizon multi-stage game with observed actions that is continuous at infinity, strategy profile s is subgame perfect if and only if there is no player i and strategy $\hat{s}_i$ that agrees with s_i except at a single stage k and h^k, and such that $\hat{s}_i$ gives a better payoff than s_i conditional on history h^k being reached.*

For a proof see [18]. We say that s satisfies the One-Stage Deviation Principle if no player can gain by deviating from s, either on or off the equilibrium path, in a single stage.

In the rest of this paper we will develop a prisoner's dilemma model for wireless networks. Such an exercise has been carried out before in other papers, but our approach and solution are quite different.

3. Network Model

We assume that nodes are selfish but not malicious. A selfish node is a rational user that wants to maximize its own welfare, defined as the benefit minus the cost of its actions. Links are assumed to be bidirectional. Wireless links are often bidirectional, and many MAC layers require bidirectional packet exchanges to avoid collisions, as is the case in IEEE 802.11. Finally, nodes are assumed to operate in promiscuous mode, so they are able to listen to all packets transmitted by their neighbors.

Forwarding a packet consumes resources. We define the normalized relaying cost to be 1. The reward a node receives if its packet is relayed is α, where we assume $\alpha \geq 1$ since the value of a packet should be at least equal to the cost of the resources used to send it. We assume that the interaction among nodes is reciprocal, i.e., any two neighbors have uniform network traffic demands and need each other to forward packets. Thus, we can isolate any pair of nodes and study the interaction between them as a two-player

Table 2: Payoff Matrix of the Packet Forwarding Game

		Node 2			
		Forward		Drop	
Node 1	Forward	$\alpha - 1$	$\alpha - 1$	$-\alpha - 1$	α
	Drop	α	$-\alpha - 1$	$-\alpha$	$-\alpha$

Table 3: Affine Transformation to the Payoff Matrix of the Packet Forwarding Game

		Node 2			
		Forward		Drop	
Node 1	Forward	1	1	$\frac{-1}{2\alpha-1}$	$\frac{2\alpha}{2\alpha-1}$
	Drop	$\frac{2\alpha}{2\alpha-1}$	$\frac{-1}{2\alpha-1}$	0	0

game. Later in Section 6 we simulate a random network with asymmetric and spatially non-uniform traffic without this assumption and test whether our conclusions still hold.

In the two-player game, one way to model the nodes is to assume that they send a packet to each other and then simultaneously decide whether to drop or forward their respective packets, and repeat this game iteratively. In this scenario the stage payoffs matrix is given in Table 2. Without loss of generality, we do an affine transformation to the payoff matrix as shown in Table 3 using the following formula: let x be any entry in Table 2, and let y be the respective entry in Table 3, then $y = (x + \alpha)/(2\alpha - 1)$. Using standard game theory notation, we will denote by $i \in \{1, 2\}$ a generic node and by $-i$ its neighbor.

Since the interaction among nodes is asynchronous in nature, we refine the game assuming that time is divided into slots and that slots last long enough to allow each node to send a sufficiently large number of packets. At the end of the slot each node finds the ratio of dropped packets by its neighbor; if the number of packets exchanged is sufficiently large, then this ratio is a good estimate of the probability of dropping a packet. This assumption is implicitly used in other papers on reputation mechanisms as well [13, 14].

Due to collisions, it is not always possible to detect whether a node forwarded a packet or not. We define $p_e \in (0,1)$ to be the probability that a packet that has been forwarded was not overheard by the originating node. We also assume that p_e is the same for both nodes. (As mentioned before, in Section 6 we test this assumption by simulating a non-uniform network to compare with our analysis.) By listening to the channel, node i then estimates the perceived dropping probability $\hat{p}_{-i}^{(k)}$ of its neighbor at time slot $k \geq 0$. It must be noted that a packet is perceived to be dropped if either $-i$ dropped it or if it is not dropped but node i did not overhear the transmission. Thus

$$\hat{p}_{-i}^{(k)} = p_{-i}^{(k)} + (1 - p_{-i}^{(k)})p_e = p_e + (1 - p_e)p_{-i}^{(k)}, \tag{1}$$

where $p_{-i}^{(k)}$ is the probability that $-i$ drops a packet.

Thus, using the payoffs of Table 3, the average payoff at time slot k is:

$$\begin{aligned} u_i^{(k)} =& (1 - p_i^{(k)})(1 - p_{-i}^{(k)}) + \frac{2\alpha}{2\alpha - 1} p_i^{(k)}(1 - p_{-i}^{(k)}) \\ & - \frac{1}{2\alpha - 1}(1 - p_i^{(k)})p_{-i}^{(k)}. \end{aligned}$$

Rearranging terms:

$$u_i^{(k)} = 1 + \frac{1}{2\alpha - 1} p_i^{(k)} - \frac{2\alpha}{2\alpha - 1} p_{-i}^{(k)}. \tag{2}$$

The discounted average payoff of player i starting from time slot n is then given by:

$$U_i^{(n)} = \sum_{k=n}^{\infty} w^{k-n} u_i^{(k)} \ , \tag{3}$$

where $w \in (0,1)$ is the discount factor. Since node i cannot know for sure $p_{-i}^{(k)}$, it does not know its payoff either. However, we use the actual payoff in the analysis since it tells us whether a given node can gain by deviating from a strategy.

Given this game, each player is allowed to use a strategy to decide whether to drop or forward packets based on the history. We use $\tilde{p}_{i\ S}^{(k)}$ to denote the dropping probability player i should use at time slot k according to strategy S. For convenience, the definitions used are given in Table 4.

Table 4: Summary of Notation

	Meaning
α	Reward a node receives if a packet has been relayed
p_e	Probability that a packet that has been forwarded was not overheard by originating node
$p_i^{(k)}$	Dropping probability of player i at time slot k
$\hat{p}_i^{(k)}$	Perceived dropping probability of player i at time slot k
$\tilde{p}_{i\ S}^{(k)}$	Dropping probability player i should use at time slot k according to strategy S
w	Discount factor. Probability that both nodes continue to interact after each time slot
$u_i^{(k)}$	Player i's average payoff at time slot k
$U_i^{(n)}$	Discounted average payoff of player i starting from time slot n

4. Analysis of Prior Proposals

To motivate our new protocol which we will present in the next section, in this section we present a few strategies that have been proposed in prior work and show their limitations.

4.1. Trigger Strategies

One idea to provide an incentive for cooperation is to develop a strategy such that the cooperation of a node is measured and if the fraction of packets it has dropped is above a threshold it is consider selfish and is disconnected for a given amount of time. Formally, a *n-step Trigger Strategy* is defined as:

$$\tilde{p}_{i\ nT}^{(0)} = 0$$
$$\tilde{p}_{i\ nT}^{(k)} = \begin{cases} 0 & if\ \hat{p}_{-i}^{(j)} \leq T\ for\ all\ j \in \{k-n, \ldots, k-1\} \\ 1 & else \end{cases}$$

where we define $\hat{p}_{-i}^{(j)} = 0$ for $j \in \mathbb{Z}_-$. From (1) it is easy to see that if node i cooperates then $\hat{p}_{-i}^{(k)} = p_e$ for all k. Hence the optimal value of $T = p_e$. In reality we cannot perfectly estimate p_e, so we have to analyze two cases:

1. If $T < p_e$ then we have that $\tilde{p}_{i\ nT}^{(k)} = 1$ for $k \geq 1$, so cooperation will never emerge.
2. If $T > p_e$ then player $-i$ will be perceived to be cooperative as long as it drops packets with probability:

$$p_{-i}^{(k)} \leq \frac{T - p_e}{1 - p_e}.$$

Therefore, since p_e is unknown, any choice of threshold other than $T = p_e$ results in either all packets being dropped or some fraction of packets being dropped. In other words, full cooperation is never the Nash equilibrium point with trigger strategies.

Variations on this strategy have been used in several reputation mechanisms, where the different proposals focus on ideas on how to detect selfish behavior and then proceed to isolate selfish nodes: Catch [14], CONFIDANT [11], OCEAN [12], and the reputation-based mechanism in [16] are among them.

4.2. Tit For Tat

A second alternative is to use a *Tit For Tat* (TFT) strategy [19]. It was generalized in [20] for the wireless context as follows:

$$\begin{aligned} \tilde{p}_{i\ TFT}^{(0)} &= 0 \\ \tilde{p}_{i\ TFT}^{(k)} &= \hat{p}_{-i}^{(k-1)} \ for\ k \geq 1. \end{aligned}$$

However, Milan *et al.* [20] proved that this strategy does not provide the right incentive either for cooperation in wireless networks.

In RMS [17] the selfishness of a node is classified into one of several different levels, and punishment is given according to the level. Such a strategy can then be considered to implement a discretized version of TFT, as opposed to the continuous version presented here.

4.3. Generous Tit For Tat

The problem with TFT is that it does not take into account the fact that it is not always possible to determine whether a packet was relayed or not

due to collisions. A way to deal with this is using a generosity factor g that allows cooperation to be restored. Such a strategy is known as *Generous TFT* (GTFT) [21] and in the case of wireless networks it can be defined [20] as follows:[1]

$$\tilde{p}_{i\ GTFT}^{(0)} = 0$$
$$\tilde{p}_{i\ GTFT}^{(k)} = \max\{\hat{p}_{-i}^{(k-1)} - g, 0\}\ for\ k \geq 1.$$

Lemma 2. *If both nodes do not deviate from the GTFT strategy then the generosity factor that maximizes the discounted average payoff is* $g^* \geq p_e$.

Proof. If $g \geq p_e$ then from (1) we have for all $k \geq 0$ and $i \in \{1, 2\}$ that $p_i^{(k)} = 0$. Using (2) and (3) we obtain:

$$U_i^{(0)} = \frac{1}{1-w}. \tag{4}$$

In the case $g < p_e$ we obtain:

$$p_i^{(0)} = 0$$

and for $k \geq 1$:

$$\begin{aligned} p_i^{(k)} &= (p_e - g) \sum_{n=0}^{k-1} (1-p_e)^n \\ &= (p_e - g) \frac{1-(1-p_e)^k}{p_e}. \end{aligned}$$

So the stage payoffs for $k \geq 1$ are:

$$u_i^{(k)} = \frac{1}{p_e} \left[g + (p_e - g)(1-p_e)^k \right].$$

Therefore the discounted average payoff is:

$$U_i^{(0)} = 1 + \frac{w}{p_e} \left[\frac{g}{1-w} + \frac{(p_e - g)(1-p_e)}{1-w(1-p_e)} \right]. \tag{5}$$

It can easily be checked that the payoff (5) is strictly less than the payoff (4). ■

[1]Note that this definition corresponds to a reputation-based mechanism, not to be confused with the credit-based mechanism proposed in [4] that bears the same name.

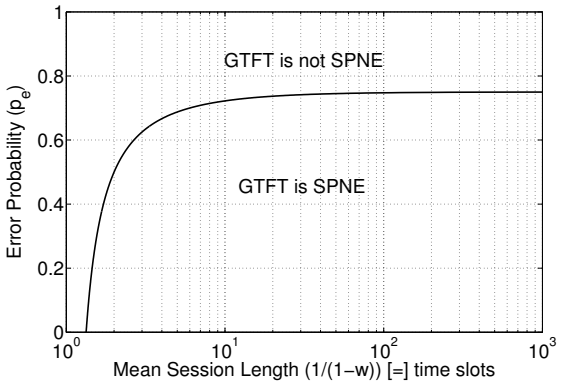

Figure 1: GTFT's Subgame Perfect Nash Equilibrium (SPNE) region for $\alpha = 2$

It is important to highlight that in the case $g > p_e$ GTFT is not a Nash equilibrium since for player $-i$ it pays to deviate dropping packets with a probability

$$p_{-i}^{(k)} \leq \frac{g - p_e}{1 - p_e}.$$

The following theorem and corollary tell us that if the interaction between two nodes lasts long enough then GTFT is a robust strategy where no node can gain by deviating from the expected behavior, even if it is not able to achieve full cooperation.

Theorem 1. *GTFT is subgame perfect if and only if*

$$g \leq p_e \text{ and } w > \frac{1}{2\alpha(1 - p_e)}.$$

(See the proof on the appendix.)

Corollary 1. *If both nodes use GTFT then cooperation is achieved on the equilibrium path if and only if $g = p_e$.*

Note that in [20] a proof was done for the case $g = p_e$ but only considering the equilibrium path. The subgame perfect region of GTFT is plotted in Fig. 1 for $\alpha = 2$. Fig. 2 shows how the shape of this region is affected by different values of α. Note that when the value of a packet grows larger

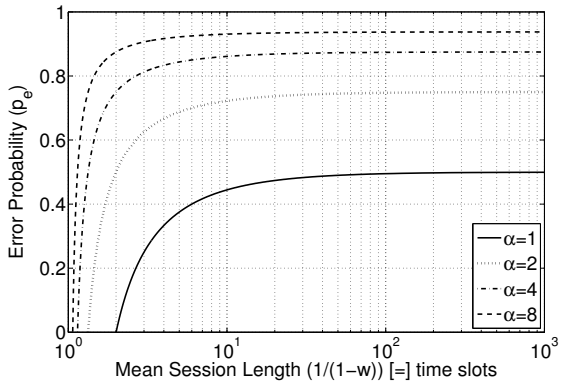

Figure 2: Sensitivity of GTFT's subgame perfect region for different values of α

compared to the actual cost of transmitting it then cooperation has a better chance to emerge since being connected is more important than reducing the cost of helping other nodes. In summary, GTFT is not satisfactory because in order to achieve full cooperation we need a perfect estimate of p_e. Such a strategy has been used in SORI [13] to punish selfish behavior.

5. DARWIN

In this section we introduce our algorithm, prove that our strategy is subgame perfect, achieves cooperation on the equilibrium path, and can cope with a group of colluding nodes. We end the section discussing some possible security issues and how they can be solved.

5.1. Definition

Our goal is to propose a reputation strategy that does not depend on a perfect estimation of p_e to achieve full cooperation and that is also more robust than previously proposed strategies. For the iterated Prisoners' Dilemma a modification of TFT known as Contrite Tit For Tat (CTFT) [22, 23] has been proposed based on the idea of contriteness: a player that made a mistake and unintentionally defected should exercise contrition and try to correct the error instead of going into a retaliation situation. This strategy depends on the notion of good standing and is defined as follows. A player

is always in good standing on the first stage. It remains in good standing as long as it cooperates when CTFT specifies that it should cooperate. If an individual is in bad standing it can get back in good standing by cooperating on one stage. Then CTFT specifies that a player should cooperate if it is in bad standing, or if its opponent is in good standing; otherwise the individual should defect. Inspired by this strategy, for the case of wireless networks we define the following strategy:

$$\tilde{p}_{i\ DARWIN}^{(k)} = \left[\gamma\left(q_{-i}^{(k-1)} - q_i^{(k-1)}\right)\right]_0^1 \ for\ k \geq 0, \tag{6}$$

where we define for $i = \{1, 2\}$:

$$q_i^{(k)} = \begin{cases} \left[\hat{p}_i^{(k)} - \tilde{p}_{i\ DARWIN}^{(k)}\right]_0^1 & for \quad k \geq 0 \\ 0 & for \quad k = -1. \end{cases} \tag{7}$$

Additionally we define the function:

$$[x]_0^1 = \begin{cases} 1 & if \quad x \geq 1 \\ x & if \quad 0 < x < 1 \\ 0 & if \quad x \leq 0 \end{cases}.$$

Recall that $\hat{p}_i^{(k)}$ denotes the estimated dropping probability and $\tilde{p}_{i\ DARWIN}^{(k)}$ is the dropping probability under DARWIN. Thus, if $\hat{p}_i^{(k)} > \tilde{p}_{i\ DARWIN}^{(k)}$, it means node i is perceived to be dropping more packets than it should under DARWIN. The parameter $q_i^{(k)}$ measures this deviation. In this case $q_i^{(k)}$ acts as a measurement of the bad standing of a node, and only the player that has better standing should proportionally punish its opponent with the *difference* in the two standings instead of the *absolute* value of the standing of its opponent. The limitation on any strategy is that it requires that the interaction between the nodes to last long enough for the reputation mechanism to be effective. This is translated in a feasible set for the parameter w, the probability that both nodes continue to interact after each time slot. In the case of DARWIN, γ determines the set of feasible values of w: the larger the punishment factor γ, up to an upper bound, the shorter the interaction between the nodes can be. This relationship will be quantitatively presented in Theorem 2.

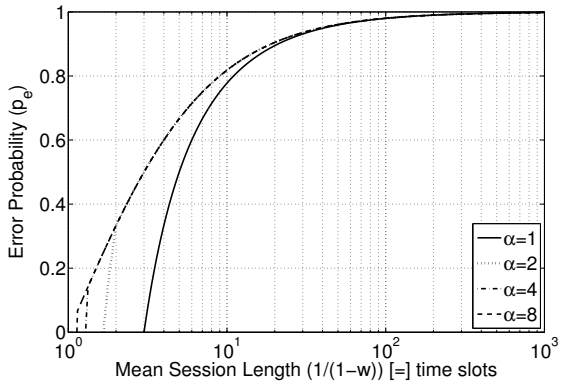

Figure 3: Sensitivity of DARWIN's subgame perfect region for different values of α assuming (9) holds

5.2. Performance Guarantees

The following theorem proves that when the interaction between two nodes lasts long enough DARWIN is a robust strategy where no node can gain by deviating from the expected behavior.

Theorem 2. *Assuming* $1 < \gamma < p_e^{-1}$*, DARWIN is subgame perfect if and only if*

$$w > \max\left\{\frac{1}{\gamma}, \frac{1}{2\alpha(1-p_e\gamma)+p_e\gamma}\right\}. \tag{8}$$

(See the proof on the appendix.)

From (8) it is clear that the optimum value of γ that minimizes this bound is a function of α and p_e. Since you cannot estimate α, a suboptimal strategy could be to choose γ to be the average of the interval $(1, p_e^{-1})$:

$$\gamma = \frac{1+p_e^{-1}}{2} = \frac{1+p_e}{2p_e}. \tag{9}$$

In Fig. 3 it is shown the subgame perfect region of DARWIN for different values of α assuming (9) holds, which is not significantly different from the subgame perfect region if we would have used the optimal value of γ.

It must be highlighted that if both nodes use DARWIN then full cooperation is achieved. This can easily be checked using (1) and the definition of DARWIN to observe the game evolution.

Lemma 3. *If both nodes use DARWIN then cooperation is achieved on the equilibrium path. That is,* $p_i^{(k)} = p_{-i}^{(k)} = 0$ *for all* $k \geq 0$.

Since this is the best any strategy S can achieve, we have that:

$$U_{i\ S}^{(0)} \leq U_{i\ DARWIN}^{(0)} \ for\ any\ strategy\ S. \tag{10}$$

It is also important to remember that for DARWIN to be subgame perfect we need to estimate p_e in order to achieve the bound $\gamma < p_e^{-1}$. Since we cannot do perfect estimation, we have that the estimated error probability $p_e^{(e)}$ is equal to

$$p_e^{(e)} = p_e + \Delta,$$

where $\Delta \in (-p_e, 1 - p_e)$ is the estimation error. If we choose γ using (9) we have:

$$\gamma = \frac{1 + p_e^{(e)}}{2p_e^{(e)}} = \frac{1 + p_e + \Delta}{2p_e + 2\Delta}.$$

So we have that $\gamma < p_e^{-1}$ if and only if:

$$\Delta > -p_e \left(\frac{1 - p_e}{2 - p_e} \right).$$

Thus, for the DARWIN strategy, one does not need a precise estimate of p_e, an estimator that overestimates p_e is sufficient for Theorem 2 to hold.

5.3. Collusion Resistance

We now consider the case when a group of colluding nodes work together to maximize their own benefit regardless of the social optimum. Define $U_{i\ S_i|S_{-i}}^{(0)}$ to be the discounted average payoff of player i using strategy S_i when it plays against player $-i$ using strategy S_{-i}. Hence (10) can be rewritten as:

$$U_{i\ S|S}^{(0)} \leq U_{i\ D|D}^{(0)} \ for\ any\ strategy\ S. \tag{11}$$

Also, a consequence of Theorem 2 is

$$U_{i\ S|D}^{(0)} < U_{i\ D|D}^{(0)} \tag{12}$$

for any strategy $S \neq$ D=DARWIN. Assume a group of colluding nodes implementing strategy S enters the network. Define $p_S \in (0, 1)$ to be the

probability that a node that implements DARWIN interacts with a colluding node. Therefore the average payoff to a cooperative node will be:

$$U(D) = p_S U^{(0)}_{i\ D|S} + (1 - p_S) U^{(0)}_{i\ D|D}.$$

Similarly, if $p_D \in (0, 1)$ is the probability that a colluding node interacts with a node implementing DARWIN we have:

$$U(S) = p_D U^{(0)}_{i\ S|D} + (1 - p_D) U^{(0)}_{i\ S|S}.$$

We have that the average payoff is bounded by

$$U(S) \leq \max \left\{ U^{(0)}_{i\ S|D}, U^{(0)}_{i\ S|S} \right\}. \tag{13}$$

So a group of colluding nodes cannot gain from unilaterally deviating if and only if $U(S) < U(D)$. Equivalently,

$$p_S \left[U^{(0)}_{i\ D|D} - U^{(0)}_{i\ D|S} \right] < U^{(0)}_{i\ D|D} - U(S). \tag{14}$$

From (11), (12) and (13) we know that

$$U^{(0)}_{i\ D|D} - U(S) \geq 0.$$

Definition 5. *Strategy S is a* naive strategy *if*

$$U^{(0)}_{i\ D|D} < U^{(0)}_{i\ D|S}. \tag{15}$$

That is, strategy S is exploited when matched against DARWIN. Furthermore, a non-naive strategy *is one such that (15) does not hold.*

From (14), we have proved the following theorem:

Theorem 3. *DARWIN is collusion resistant against a naive strategy. Furthermore, it is resistant against a non-naive strategy if and only if*

$$p_S < \frac{U^{(0)}_{i\ D|D} - U(S)}{U^{(0)}_{i\ D|D} - U^{(0)}_{i\ D|S}}.$$

Thus if cooperative nodes mostly interact among each other then DARWIN can resist group attacks.

5.4. Security Issues

In this section, we will comment on possible security issues in implementing DARWIN. Since our solutions to these issues rely on other works, our discusion will be brief.

5.4.1. Short Term Identities and Sybil Attacks

Nodes can change identities to avoid detection or to help spread false values to improve their own reputation. To cope with this we can use a proof-of-effort approach, first suggested for ad hoc networks in [12]: a node that claims to be entering the network for the first time must show that it has spent some effort creating its identity, otherwise it is not allowed to connect. Since memory access speeds vary across machines much less than CPU speeds, it is used a memory-bound function [24, 25]. The main two properties it has is that its computing time is determined by the memory access speed and not the CPU speed, and that it is moderately hard to compute but very easy to verify. This approach tends to be more egalitarian and tries to avoid the problem selfish users with high-end computers pose to the network, since they could potentially spend less CPU time with the burden of creating new identities.

5.4.2. Node Impersonation

Selfish nodes can try to impersonate cooperative nodes in order to boost their reputation or to request other nodes to forward their own packets. This problem can be solved generating a shared secret key among each pair of nodes and using it in conjunction with a Message Authentication Code. The key can be safely exchanged over an insecure channel using the Diffie-Hellman key exchange algorithm [26].

6. Simulations

In this section we first present a possible implementation of our reputation mechanism and later we will present the settings and results of our simulation study of the performance of DARWIN against the strategies studied in Section 4.

6.1. Algorithm Implementation

Let $N_i^{(k)}$ denote the set of one hop neighbors that node i has discovered in time interval k by overhearing packet transmissions. For every node $j \in N_i^{(k)}$

node i keeps two counters, one for the number of messages sent to j for forwarding ($S_{ij}^{(k)}$) in time slot k and another for the number of messages j actually forwarded ($F_{ij}^{(k)}$) in time interval k. At the end of the time slot it computes the ratio

$$c_{ij}^{(k)} = \frac{F_{ij}^{(k)}}{S_{ij}^{(k)}}$$

and proceeds to send $c_{ij}^{(k)}$ to its neighbors. With the values gathered node i estimates j's average connectivity ratio

$$\hat{c}_j^{(k)} = \frac{\sum\limits_{\substack{m \in N_i^{(k)} \cup \{i\} \\ m \neq j}} c_{im}^{(k)} \times c_{mj}^{(k)}}{\sum\limits_{\substack{m \in N_i^{(k)} \cup \{i\} \\ m \neq j}} c_{im}^{(k)}},$$

where by definition $c_{ii}^{(k)} = 1$ for all k. It must be noted that the average is weighted with the perceived connectivity ratio that node i measured from node m. This helps to avoid sybil attacks to spread false values with the hope to improve a selfish node's reputation since all its other identities have low connectivity too, so they have a small impact on the average. In a similar way, node i will find $\hat{c}_i^{(k)}$, the average connectivity ratio its one-hop neighborhood perceived from it during time slot k. We define $\hat{p}_j^{(k)} = 1 - \hat{c}_j^{(k)}$ and use (6) and (7) to find the dropping probability that node i will use while forwarding packets for node j in time interval $k+1$.

Since we need $\gamma < p_e^{-1}$, we need to estimate p_e. An interesting solution was proposed in [14] probing a node with anonymous messages, but it increases the overhead of the protocol. Instead, note that p_e is the probability that at least one terminal in $N_i^{(k)}$ transmits when node j transmits. Thus we estimate p_e by measuring the fraction of time at least one node different from j transmits. Call it $\hat{p}_{ej}$. Mathematically, if $T_j^{(k)}$ is the fraction of time node j has transmitted up to time interval k and $T_c^{(k)}$ is the fraction of time a collision occurred up to time interval k we have:

$$\hat{p}_{ej} = T_c^{(k)} + \sum_{\substack{n \in N_i^{(k)} \\ n \neq j}} T_n^{(k)}.$$

In case the MAC layer uses a CSMA/CA protocol, and due to the exposed terminal problem, we will have that $\hat{p}_{ej} \geq p_e$. This overestimation is not a problem for our algorithm since

$$\gamma < \frac{1}{\hat{p}_{ej}} \leq \frac{1}{p_e}.$$

6.2. Settings

Our goal is to study the network performance of the different strategies presented in Section 4 and how they compare against DARWIN. To do that we used the network simulator *ns-2*. For the propagation we used the two-ray ground reflection model, while the IEEE 802.11 Distributed Coordination Function (DCF) was used at the MAC layer. Nodes had a physical radio range of 250 m and a raw bandwidth of 2 Mbps. Routing was performed by the Dynamic Source Routing (DSR) protocol. We simulated a network of 50 nodes randomly placed in an area of $670 \times 670\ m^2$ that implement a reputation mechanism in a given simulation run, where we randomly selected five nodes that do not implement such strategy and behave selfishly dropping all packets that are not destined to them. In the rest of this section, a selfish node will be taken to mean a node that does not implement the reputation mechanism and a cooperative node one which does. Unless otherwise noted, there are 14 source-destination pairs and each source transmits at a Constant Bit Rate (CBR) of 2 packets/s, with a packet size of 512 bytes. The simulation time is 800 s, where the time intervals used were 60 seconds long. Each figure presented is the average of 120 randomly generated runs.

Since our goal is to study the different strategies and not specific implementations, all cooperative nodes use the implementation suggested in Section 6.1 to test node behavior and share reputation values. The only difference is on the strategy used to punish selfish behavior. For the case when nodes implement the n-step Trigger strategy, the threshold T is set to be 0.2, while $n = 5$. For GTFT we set the parameter g to be 0.1, while for DARWIN we set γ to be 2.

6.3. Results

Before presenting the results of our simulation study, we would like to emphasize the fact that, as proved in Sections 4 and 5, DARWIN can help restore cooperation under a larger set of conditions on nodes interactions, is more robust against imperfect knowledge of network parameters compared

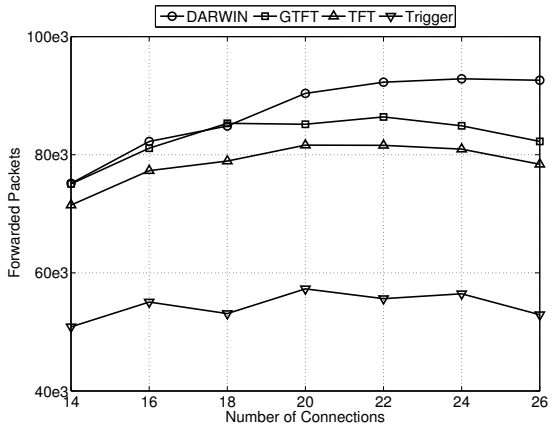

Figure 4: Number of forwarded packets for different numbers of source-destination pairs

to other strategies, and is a self enforcing strategy where no node or group of colluding nodes can obtain a gain from deviating from our strategy. These desirable characteristics for any reputation mechanism mean that the chances that a rational user deviates from DARWIN and behaves selfishly are smaller compared to the other strategies studied, which is the ultimate goal of a mechanism that tries to incentivize cooperation. The simulations complement these theoretical conclusions by assuming that some nodes are rogue users and behave selfishly.

To evaluate network performance, we measure the total number of forwarded packets. In Figure 4 we explore the effect of varying the total number of source-destination pairs. As it can be seen, the throughput gap for cooperative nodes increases with the number of connections. The reason for this is that when there are more active connections the probability that a node does not listen when a packet is being forwarded increases, leading to an increased number of misunderstandings where cooperative nodes are deemed to be acting as selfish. This increases the level of retaliation situations in TFT and the n-step Trigger strategies. It can be noted that when the number of connections is greater than 18 there is a decrease in throughput in GTFT compared to DARWIN. As explained in Section 4.3, GTFT requires a perfect estimation of the probability p_e that a packet that has been forwarded was not overheard by the originating node to achieve full cooperation. Since we keep constant the generosity factor g in our simulations, once $p_e > g$ when

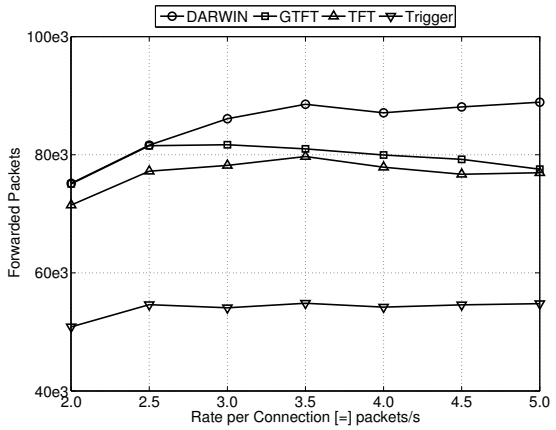

Figure 5: Number of forwarded packets for different connection rates (for a packet size of 512 bytes)

the number of connections is large enough, we have that network throughput starts to decrease. This behavior is also evident in Figure 5, where the relationship between source rate and the number of forwarded packets is presented. Since DARWIN does not require a perfect estimate of p_e but an overestimation suffices, as explained in Section 5.2, and since it compensates for the misunderstandings between cooperative nodes, we see that the advantage of using DARWIN over other strategies is more apparent when the network becomes heavily congested.

Figure 6 explores the impact of the fraction of selfish nodes, where the figure presented is the average of 240 randomly generated runs instead of 120 as the rest of the plots, showing the average number of forwarded packets per node for both selfish and cooperative nodes. This was done because the confidence intervals for this plot tended to be larger than for the other plots when we only used 120 runs. Since the goal of this plot is to highlight the difference in throughput between cooperative and selfish nodes, and not the throughput difference between competing strategies as it has already been studied in Figures 4 and 5, we run our simulations in the low traffic regime.

As expected, the total throughput of cooperative nodes decreased proportionally when the number of selfish nodes increases. This is due to the fact that since the number of selfish nodes increases, the total number of packets being dropped increases proportionally. In this case, it can be seen that the

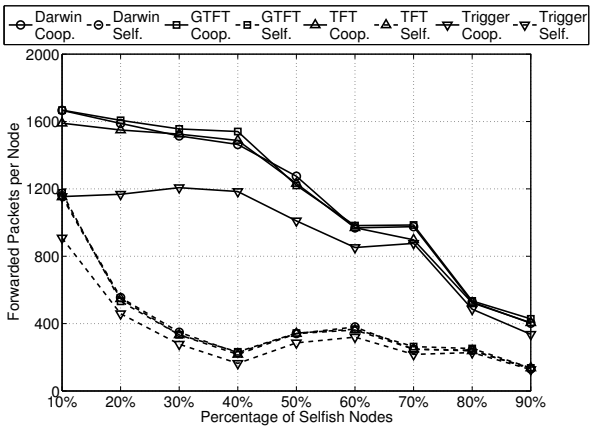

Figure 6: Number of forwarded packets per node for different numbers of selfish nodes

average number of forwarded packets for cooperative nodes is larger than the one for selfish nodes, even when 90% of the nodes act selfishly. The fact that the difference between the throughput decreases is less relevant than the fact that selfishness does not improve performance. It can also be noted that of all the strategies simulated the n-step Trigger is the one that has the harshest punishment for selfish behavior, but at the cost of significantly decreasing network throughput for cooperative nodes.

In Figure 7 we study the effect of mobility on the effectiveness of the punishment mechanisms, where the sources transmit at a rate of 4 packets/s. The mobility model used is the random waypoint model, where a node moves to a random destination at a speed uniformly distributed between 0 to 20 m/s, and once it reaches the destination it remains there for a specified pause time before choosing its next destination. To complement our simulation study, in this figure we include in the comparison CORE [10, 15]. As can be observed, the more the nodes move the less throughput nodes get, since the routing algorithm sends packets to stalled routes, which eventually leads to packet dropping. However, the performance gap of DARWIN compared to the other strategies remains the same, showing that the mechanism is better able to incentivize cooperation even in the case when nodes roam.

In summary, nodes that are selfish are punished similarly by most protocols, but nodes that implement DARWIN get much better throughput than nodes that implement n-step Trigger or TFT strategies. Furthermore, the

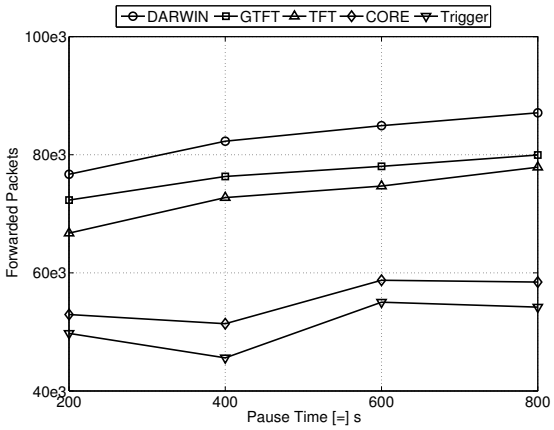

Figure 7: Number of forwarded packets per node for different pause times

throughput of DARWIN is better in heavily loaded networks compared to nodes that implement GTFT.

One important aspect of every protocol is the overhead that results from its implementation. Figure 8 explores this for different source rates when all nodes implement DARWIN compared to the same network when all nodes are cooperative and do not run DARWIN. DARWIN (and any other reputation mechanism for that matter) incurs a certain fixed overhead associated with sharing and processing reputation information, thus, as is to be expected, the fraction of overhead packets to data packets is higher at low loads but smaller at high loads. This feature is desirable since resources are at a premium at high loads.

7. Related Work

Incentive mechanisms can be broadly divided in two categories, according to the techniques they use to enforce cooperation: credit-based schemes and reputation-based schemes. Here we present a review of the previous work done in both areas.

7.1. Credit-Based Schemes

The strategy proposed in [6] is based on a nuglet counter that increases every time a node forwards a packet, and is decreased by the estimated number of intermediate nodes every time a packet is sent. A node is only allowed

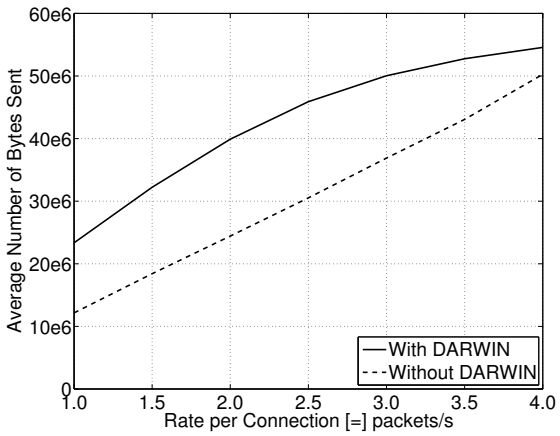

Figure 8: Overhead of DARWIN

to send a packet if its nuglet counter will remain positive after the operation. Therefore, if a node wants to be able to transmit it has to cooperate. This scheme requires tamper resistant hardware, but this kind of hardware must be trusted with caution [27]. Sprite [5] avoids the use of tamper resistant hardware by storing receipts of forwarded packets, and later they are cleared with a central trusted authority that distributes the credits to cooperative nodes. The drawback is the need of an infrastructure to operate, which may hinder its ability to gain widespread acceptance, e.g., in post-disaster networks.

An algorithm called Generous Tit For Tat (GTFT) has been proposed in [4]: a node accepts to forward packets in a session if and only if the throughput received by the node from the network so far is greater than the throughput given to the network minus a generosity factor; if a node decides to reject a session, it informs the source so it can establish another path. Assuming that misbehaving nodes do not lie about their actual actions, [4] proved that no node has an incentive to unilaterally deviate from the GTFT strategy.

In [7], a pricing mechanism is studied through fluid-level simulations. It has been demonstrated that users' prices and credit balances stabilize for fixed ad hoc networks, where nodes in the center of the network have an advantage since they can act as relay nodes for a larger number of routes. Ad hoc-VCG [8] is a reactive routing protocol that implements a variation of

the VCG mechanism. As is mentioned in [8], the protocol has considerable overhead on the route discovery phase if communication sessions between two nodes are usually short or the routing path frequently changes during a session; additionally, to guarantee truthfulness and cost-efficiency it is required that every node has complete and up-to-date knowledge of the underlying graph, so techniques such as route caches are not suitable with this protocol.

7.2. Reputation-Based Schemes

In [9] the reputation mechanism performs two functions: (i) identifies misbehaving nodes by monitoring packet forwarding, and (ii) helps the routing protocol avoid those nodes by informing the source node that there are selfish nodes on its path. The source node can use this information to find alternate paths. Hence, the mechanism only tries to avoid selfish nodes, but the behavior is not discouraged. CONFIDANT [11] goes one step further and after a selfish node is detected, it is isolated; however, it relies on building a "friends" list that is imprinted in every node on a user-to-user basis.

In SORI [13] and Catch [14] the spreading of reputation information is limited to one-hop neighbors. SORI evaluates the reputation of a node by weighting the information of all its neighbors and then punishes it, if necessary, with a Generous Tit-For-Tat strategy. Catch uses control messages to reduce the impact of collisions on estimating reputation, and to punish selfish behavior it relies on a trigger strategy.

CORE [10, 15] keeps a counter to keep track of the neighbor's last B actions, where the counter is increased by 1 every time the node cooperates, and it is decreased by 1 every time it defects. If the counter is positive, CORE will cooperate, otherwise it will punish its neighbor by defecting.

8. Conclusions

In this paper we have studied how reputation-based mechanisms can help cooperation emerge among selfish users. We first showed the properties of previously proposed schemes, and with the insight gained from such understanding, we proposed a new mechanism called DARWIN. We showed that DARWIN is robust to imperfect measurements, is also collusion-resistant and is able to achieve full cooperation. We also showed that the algorithm is relatively insensitive to parameter choices. Simulation results complement our

theoretical analysis, and show that DARWIN can achieve a higher throughput than any of the other strategies we studied; furthermore, we showed that DARWIN can be implemented with low overhead.

It must be noted that in the definition of DARWIN it is assumed that nodes share the perceived dropping probability with each other. This assumption is made in order to facilitate the theoretical analysis by isolating a pair of nodes, but in an implementation a mechanism is required to guarantee that even if a node lies, the reputation scheme still works. To do that we must rely on other cooperative nodes to tell the actual perceived dropping probability of a node in order to minimize the impact of liars, and the average of the received values is the one to be used in this reputation scheme. In [28, 29] it is proved that if the connectivity of the network is at least $2f + 1$, then using linear iterations it is possible for all nodes to share some initial values to calculate an arbitrary function on them when there are up to f malicious nodes in the network. In principle, such a scheme can be used in our problem. However, the study of this in the context of wireless networks is an interesting challenge and is a good topic for future research.

9. Appendix

Here we present the proofs of the theorems presented in this paper.

THEOREM 1. *GTFT is subgame perfect if and only if*

$$g \leq p_e \text{ and } w > \frac{1}{2\alpha(1-p_e)}.$$

PROOF. In Section 4.3 we have already seen that if $g > p_e$ then GTFT is not a Nash equilibrium, so for the rest of the proof we will assume $g \leq p_e$. It must be noted that GTFT is a one-stage history strategy because it only needs to take into account what happened in the previous stage. With that in mind, and without loss of generality, let us assume that any history h^n is represented as $p_i^{(0)} = p_i$ for $i \in \{1, 2\}$. If both nodes use GTFT then using (1) we have the following subgame evolution:

k	$p_i^{(k)}$
0	p_i
1	$p_{-i}(1-p_e)+p_e-g$
2	$p_i(1-p_e)^2+(p_e-g)\sum_{n=0}^{1}(1-p_e)^n$
3	$p_{-i}(1-p_e)^3+(p_e-g)\sum_{n=0}^{2}(1-p_e)^n$
$\vdots$	$\vdots$

or equivalently for $k \geq 1$:

$$p_i^{(k)} = \theta_i^{(k)}(1-p_e)^k + \frac{(p_e-g)}{p_e}\left[1-(1-p_e)^k\right]$$

where

$$\theta_i^{(k)} = \begin{cases} p_i & if\ k\ is\ even \\ p_{-i} & if\ k\ is\ odd. \end{cases}$$

Therefore from (2) the stage payoffs for $k \geq 1$ are:

$$u_i^{(k)} = 1 + \frac{1}{2\alpha-1}p_i^{(k)} - \frac{2\alpha}{2\alpha-1}p_{-i}^{(k)}.$$

If player i deviates at stage 1 using

$$p_{i\delta}^{(1)} = \tilde{p}_{i\ GTFT}^{(1)} + \delta$$

for some $\delta > 0$ and later conforms to GTFT, we have the following dropping probabilities:

k	$p_{i\delta}^{(k)}$
0	p_i
1	$p_{-i}(1-p_e)+(p_e-g)+\delta$
2	$p_i(1-p_e)^2+(p_e-g)\sum_{n=0}^{1}(1-p_e)^n$
3	$p_{-i}(1-p_e)^3+(p_e-g)\sum_{n=0}^{2}(1-p_e)^n+\delta(1-p_e)^2$
$\vdots$	$\vdots$

or equivalently:

$$p_{i\delta}^{(2m+1)} = p_{-i}(1-p_e)^{2m+1} + \frac{(p_e-g)}{p_e}\left[1-(1-p_e)^{2m+1}\right] + \delta(1-p_e)^{2m}$$

$$p_{i\delta}^{(2m)} = p_i(1-p_e)^{2m} + \frac{(p_e - g)}{p_e}\left[1-(1-p_e)^{2m}\right].$$

So we have:

$$p_{i\delta}^{(2m+1)} = p_i^{(2m+1)} + \delta(1-p_e)^{2m} \; for \; m \geq 0$$
$$p_{i\delta}^{(2m)} = p_i^{(2m)} \; for \; m \geq 1.$$

Which leads to the following stage payoffs:

$$u_{i\delta}^{(2m+1)} = u_i^{(2m+1)} + \frac{1}{2\alpha - 1}\delta(1-p_e)^{2m} \; for \; m \geq 0$$

$$u_{i\delta}^{(2m)} = u_i^{(2m)} - \frac{2\alpha}{2\alpha - 1}\delta(1-p_e)^{2m-1} \; for \; m \geq 1.$$

Since the stage payoff received at stage 0 is independent of the action player i takes at stage 1, we are only interested in finding the following discounted average payoff:

$$\begin{aligned} U_{i\delta}^{(1)} &= \sum_{k=1}^{\infty} w^{k-1} u_{i\delta}^{(k)} \\ &= U_i^{(1)} + \frac{\delta\left[1 - 2\alpha w(1-p_e)\right]}{(2\alpha - 1)\left[1 - w^2(1-p_e)^2\right]}. \end{aligned}$$

Where $U_i^{(1)}$ is the discounted payoff received if $\delta = 0$. Since we assume that $\alpha \geq 1$, it does not pay to deviate if:

$$1 - 2\alpha w(1-p_e) < 0.$$

But this is true if and only if:

$$w > \frac{1}{2\alpha(1-p_e)}.$$

Then by the One-Stage Deviation Principle GTFT is subgame perfect. ■

THEOREM 2. *Assuming $1 < \gamma < p_e^{-1}$, DARWIN is subgame perfect if and only if*

$$w > \max\left\{\frac{1}{\gamma}, \frac{1}{2\alpha(1-p_e\gamma) + p_e\gamma}\right\}.$$

PROOF. The line of reasoning is similar to the one presented for Theorem 1. DARWIN is a one-stage history strategy because it only needs to take into account what happened in the previous stage. Hence, and without loss of generality, any history h^n can be represented as $q_i^{(0)} = q_i$ for $i \in \{1, 2\}$. If both nodes do not deviate from DARWIN then using (1) we have for $k \geq 1$ the following subgame evolution:

If $q_i \geq q_{-i}$ then:

$$\begin{aligned}
p_i^{(k)} &= 0 \\
p_{-i}^{(k)} &= p_e^{k-1}\gamma^{k-1}\min\{1, \gamma(q_i - q_{-i})\} \\
\hat{p}_i^{(k)} &= p_e \\
\hat{p}_{-i}^{(k)} &= p_e + p_e^{k-1}\gamma^{k-1}(1 - p_e)\min\{1, \gamma(q_i - q_{-i})\} \\
q_i^{(k)} &= p_e \\
q_{-i}^{(k)} &= p_e - p_e^{k}\gamma^{k-1}\min\{1, \gamma(q_i - q_{-i})\}
\end{aligned}$$

From (2) the stage payoffs for $k \geq 1$ are:

$$u_{i\ a}^{(k)} = 1 - \frac{2\alpha}{2\alpha - 1}\left[(p_e\gamma)^{k-1}\min\left\{1, \gamma(q_i - q_{-i})\right\}\right].$$

If $q_i < q_{-i}$ then:

$$\begin{aligned}
p_i^{(k)} &= p_e^{k-1}\gamma^{k-1}\min\{1, \gamma(q_{-i} - q_i)\} \\
p_{-i}^{(k)} &= 0 \\
\hat{p}_i^{(k)} &= p_e + p_e^{k-1}\gamma^{k-1}(1 - p_e)\min\{1, \gamma(q_{-i} - q_i)\} \\
\hat{p}_{-i}^{(k)} &= p_e \\
q_i^{(k)} &= p_e - p_e^{k}\gamma^{k-1}\min\{1, \gamma(q_{-i} - q_i)\} \\
q_{-i}^{(k)} &= p_e
\end{aligned}$$

From (2) the stage payoffs for $k \geq 1$ are:

$$u_{i\ b}^{(k)} = 1 + \frac{1}{2\alpha - 1}p_e^{k-1}\gamma^{k-1}\min\left\{1, \gamma(q_{-i} - q_i)\right\}.$$

If player i deviates at stage 1 using

$$p_{i\delta}^{(1)} = \tilde{p}_{i\ DARWIN}^{(1)} + \delta$$

for some $\delta > 0$ and later conforms to DARWIN, we have the following game evolution:

If $q_i \geq q_{-i}$ then:

$$
\begin{aligned}
p_i^{(1)} &= \delta \\
p_i^{(k)} &= 0 \\
p_{-i}^{(1)} &= \min\{1, \gamma(q_i - q_{-i})\} \\
p_{-i}^{(k)} &= (p_e\gamma)^{k-2} \min\{1, \gamma\delta(1-p_e) + p_e\gamma p_{-i}^{(1)}\} \\
\hat{p}_i^{(1)} &= p_e + \delta(1-p_e) \\
\hat{p}_i^{(k)} &= p_e \\
\hat{p}_{-i}^{(1)} &= p_e + (1-p_e)p_{-i}^{(1)} \\
\hat{p}_{-i}^{(k)} &= p_e + (p_e\gamma)^{k-2}(1-p_e) \min\{1, \gamma\delta(1-p_e) + p_e\gamma p_{-i}^{(1)}\} \\
q_i^{(1)} &= p_e + \delta(1-p_e) \\
q_i^{(k)} &= p_e \\
q_{-i}^{(1)} &= p_e - p_e p_{-i}^{(1)} \\
q_{-i}^{(k)} &= p_e - p_e^{k-1}\gamma^{k-2} \min\{1, \gamma\delta(1-p_e) + p_e\gamma p_{-i}^{(1)}\}
\end{aligned}
$$

Therefore from (2) the stage payoffs are:

$$u_{i\delta}^{(1)} = u_{i\ a}^{(1)} + \frac{\delta}{2\alpha - 1}$$

$$u_{i\delta}^{(k)} = u_{i\ a}^{(k)} - \frac{2\alpha(p_e\gamma)^{k-2}}{2\alpha - 1} \min\{1 - p_e\gamma p_{-i}^{(1)}, \gamma\delta(1-p_e)\}.$$

Since the stage payoff received at stage 0 is independent of the action player i takes at stage 1, we are only interested in finding the discounted average payoff

$$
\begin{aligned}
U_{i\delta}^{(1)} &= \sum_{k=1}^{\infty} w^{k-1} u_{i\delta}^{(k)} \\
&= U_{i\ a}^{(1)} + \frac{1}{2\alpha - 1}\left[\delta - \frac{2\alpha w}{1 - wp_e\gamma} \min\{1 - p_e\gamma p_{-i}^{(1)}, \gamma\delta(1-p_e)\}\right],
\end{aligned}
$$

where $U_{i\ a}^{(1)}$ is the discounted payoff received if $\delta = 0$. It does not pay to deviate if $U_{i\delta}^{(1)} < U_{i\ a}^{(1)}$. Since we assume that $\alpha \geq 1$, we only have to check two cases:

1. If $1 - p_e\gamma p_{-i}^{(1)} < \gamma\delta(1-p_e)$ we need the following condition

$$\delta - \frac{2\alpha w(1 - p_e\gamma p_{-i}^{(1)})}{1 - wp_e\gamma} < 0$$

to be true for any δ. Equivalently:

$$w > \max_{0 \leq \delta \leq 1} \left\{ \frac{\delta}{2\alpha(1 - p_e\gamma p_{-i}^{(1)}) + p_e\gamma\delta} \right\}.$$

So we get the bound:

$$w > \frac{1}{2\alpha(1 - p_e\gamma p_{-i}^{(1)}) + p_e\gamma}. \tag{16}$$

2. If $1 - p_e\gamma p_{-i}^{(1)} \geq \gamma\delta(1 - p_e)$ we need the following condition:

$$\delta - \frac{2\alpha w\gamma\delta(1 - p_e)}{1 - wp_e\gamma} < 0.$$

Thus we have the bound:

$$w > \frac{1}{2\alpha\gamma(1 - p_e) + p_e\gamma}. \tag{17}$$

For the case $q_i < q_{-i}$ the analysis has to be more detailed. In stage 1 according to DARWIN player i has to drop player $-i$'s packets with probability:

$$\tilde{p}_{i\ DARWIN}^{(1)} = \min\{1, \gamma(q_{-i} - q_i)\}.$$

So if $\gamma \geq \frac{1}{q_{-i} - q_i}$ then player i cannot deviate at stage 1 for any value of w. In the case that $\gamma < \frac{1}{q_{-i} - q_i}$ we can only increase δ up to:

$$\delta \leq 1 - \gamma(q_{-i} - q_i).$$

Now the rest of the analysis will consider the following two cases:

$$\delta \leq \min\left\{1 - \gamma(q_{-i} - q_i), \frac{p_e\gamma(q_{-i} - q_i)}{1 - p_e}\right\} \tag{18}$$

$$\frac{p_e\gamma(q_{-i} - q_i)}{1 - p_e} < \delta \leq 1 - \gamma(q_{-i} - q_i) \tag{19}$$

For the case when (18) is true we have the following evolution of the game:

$$
\begin{aligned}
p_i^{(1)} &= \gamma(q_{-i} - q_i) + \delta \\
p_i^{(k)} &= p_e^{k-1}\gamma^k(q_{-i} - q_i) - \delta p_e^{k-2}\gamma^{k-1}(1 - p_e) \\
p_{-i}^{(1)} &= 0 \\
p_{-i}^{(k)} &= 0 \\
\hat{p}_i^{(1)} &= p_e + \gamma(q_{-i} - q_i)(1 - p_e) + \delta(1 - p_e) \\
\hat{p}_i^{(k)} &= p_e + p_e^{k-1}\gamma^k(q_{-i} - q_i)(1 - p_e) - \delta p_e^{k-2}\gamma^{k-1}(1 - p_e)^2 \\
\hat{p}_{-i}^{(1)} &= p_e \\
\hat{p}_{-i}^{(k)} &= p_e \\
q_i^{(1)} &= p_e - p_e\gamma(q_{-i} - q_i) + \delta(1 - p_e) \\
q_i^{(k)} &= p_e - p_e^k\gamma^k(q_{-i} - q_i) + \delta p_e^{k-1}\gamma^{k-1}(1 - p_e) \\
q_{-i}^{(1)} &= p_e \\
q_{-i}^{(k)} &= p_e
\end{aligned}
$$

In this case, and from (2), the stage payoffs are:

$$u_{i\delta}^{(1)} = u_{i\ b}^{(1)} + \frac{\delta}{2\alpha - 1}$$

$$u_{i\delta}^{(k)} = u_{i\ b}^{(k)} - \frac{\delta p_e^{k-2}\gamma^{k-1}(1 - p_e)}{2\alpha - 1}.$$

And the discounted average payoff starting from stage 1 is:

$$U_{i\delta}^{(1)} = \sum_{k=1}^{\infty} w^{k-1}u_{i\delta}^{(k)} = U_{i\ b}^{(1)} + \frac{\delta}{2\alpha - 1}\left[1 - \frac{w\gamma(1 - p_e)}{1 - wp_e\gamma}\right].$$

Since $\alpha \geq 1$ it does not pay to deviate if:

$$1 - \frac{w\gamma(1 - p_e)}{1 - wp_e\gamma} < 0.$$

Which leads to the following bound on w:

$$w > \frac{1}{\gamma}. \tag{20}$$

For the case when (19) is true we have the following game evolution:

$$
\begin{aligned}
p_i^{(1)} &= \gamma(q_{-i} - q_i) + \delta \\
p_i^{(k)} &= 0 \\
p_{-i}^{(1)} &= 0 \\
p_{-i}^{(k)} &= p_e^{k-2}\gamma^{k-2}\min\{1, \gamma\delta(1-p_e) - p_e\gamma^2(q_{-i} - q_i)\} \\
\hat{p}_i^{(1)} &= p_e + \gamma(q_{-i} - q_i)(1-p_e) + \delta(1-p_e) \\
\hat{p}_i^{(k)} &= p_e \\
\hat{p}_{-i}^{(1)} &= p_e \\
\hat{p}_{-i}^{(k)} &= p_e + (1-p_e)p_{-i}^{(k)} \\
q_i^{(1)} &= p_e - p_e\gamma(q_{-i} - q_i) + \delta(1-p_e) \\
q_i^{(k)} &= p_e \\
q_{-i}^{(1)} &= p_e \\
q_{-i}^{(k)} &= p_e - p_e p_{-i}^{(k)}
\end{aligned}
$$

From (2), the respective stage payoffs are:

$$u_{i\delta}^{(1)} = u_{i\ b}^{(1)} + \frac{\delta}{2\alpha - 1}$$

$$u_{i\delta}^{(k)} = u_{i\ b}^{(k)} - \frac{(p_e\gamma)^{k-2}}{2\alpha - 1}\left[p_e\gamma^2(q_{-i} - q_i) + 2\alpha\min\{1, \gamma\delta(1-p_e) - p_e\gamma^2(q_{-i} - q_i)\}\right].$$

The discounted average payoff starting from stage 1 is:

$$
\begin{aligned}
U_{i\delta}^{(1)} &= \sum_{k=1}^{\infty} w^{k-1}u_{i\delta}^{(k)} \\
&= U_{i\ b}^{(1)} + \frac{1}{2\alpha - 1}\left\{\delta - \frac{w\left[p_e\gamma^2 Q + 2\alpha\min\{1, \gamma\delta(1-p_e) - p_e\gamma^2 Q\}\right]}{1 - wp_e\gamma}\right\}.
\end{aligned}
$$

Where $Q = q_{-i} - q_i$ and $U_{i\ b}^{(1)}$ is the discounted payoff received if player i does not deviate. It does not pay to deviate if $U_{i\delta}^{(1)} < U_{i\ b}^{(1)}$. Since we assume $\alpha \geq 1$, we have:

1. If $\gamma\delta(1-p_e) - p_e\gamma^2(q_{-i} - q_i) > 1$ we need the condition

$$\delta - \frac{w[2\alpha + p_e\gamma^2(q_{-i} - q_i)]}{1 - wp_e\gamma} < 0$$

to be true for any δ. Equivalently:

$$w > \max_{\delta}\left\{\frac{\delta}{2\alpha + p_e\gamma^2(q_{-i} - q_i) + p_e\gamma\delta}\right\}.$$

Since δ is bounded by (19) we get:

$$w > \frac{1-\gamma(q_{-i}-q_i)}{2\alpha + p_e\gamma^2(q_{-i}-q_i) + p_e\gamma[1-\gamma(q_{-i}-q_i)]}.$$

Simplifying:

$$w > \frac{1-\gamma(q_{-i}-q_i)}{2\alpha + p_e\gamma}. \tag{21}$$

2. If $\gamma\delta(1-p_e) - p_e\gamma^2(q_{-i}-q_i) \leq 1$ we need the following condition:

$$\delta - \frac{w\left[p_e\gamma^2 Q + 2\alpha\gamma\delta(1-p_e) - 2\alpha p_e\gamma^2 Q\right]}{1-wp_e\gamma} < 0.$$

Where Q was defined above. Thus we have the bound:

$$w > \max_{\delta}\left\{\frac{\delta}{\delta\left[2\alpha\gamma(1-p_e)+p_e\gamma\right] - (2\alpha-1)p_e\gamma^2 Q}\right\}.$$

Since δ is bounded by (19) we get:

$$w > \frac{1}{\gamma}. \tag{22}$$

So for a given history h^n we have found five bounds that w has to fulfill in order for DARWIN to be a Nash equilibrium in a given subgame. We first start noting that (20) and (22) are identical, so we really have four bounds, two of which are dependent on h^n. In order to find the conditions under which DARWIN is subgame perfect we need to find bounds that are history independent. In the case of (16) the bound is maximized by:

$$w > \frac{1}{2\alpha(1-p_e\gamma) + p_e\gamma}. \tag{23}$$

Similarly, (21) is maximized by:

$$w > \frac{1}{2\alpha + p_e\gamma}. \tag{24}$$

Comparing (17), (23) and (24) it is easy to check that (23) is the strictest bound since we assumed $\gamma > 1$. In summary, we have the following bound on w for DARWIN:

$$w > \max\left\{\frac{1}{\gamma}, \frac{1}{2\alpha(1-p_e\gamma) + p_e\gamma}\right\}.$$

Thus if the bound holds true, by the One-Stage Deviation Principle DARWIN is subgame perfect. ■

Acknowledgements

Research supported by Motorola through the Motorola Center for Communication.

References

[1] J. J. Jaramillo, R. Srikant, DARWIN: Distributed and adaptive reputation mechanism for wireless ad-hoc networks, in: Proc. 13th Annual International Conference on Mobile Computing and Networking (Mobicom), Montreal, Canada, 2007, pp. 87–97.

[2] L. Buttyán, J.-P. Hubaux, Enforcing service availability in mobile ad-hoc WANs, in: Proc. International Symposium on Mobile Ad Hoc Networking & Computing (MobiHoc '00), Boston, MA, 2000, pp. 87–96.

[3] V. Srinivasan, P. Nuggehalli, C. F. Chiasserini, R. R. Rao, Energy efficiency of ad hoc wireless networks with selfish users, in: Proc. European Wireless Conference, Florence, Italy, 2002.

[4] V. Srinivasan, P. Nuggehalli, C. F. Chiasserini, R. R. Rao, Cooperation in wireless ad hoc networks, in: Proc. IEEE INFOCOM '03, Vol. 2, San Francisco, CA, 2003, pp. 808–817.

[5] S. Zhong, J. Chen, Y. R. Yang, Sprite: A simple, cheat-proof, credit-based system for mobile ad-hoc networks, in: Proc. IEEE INFOCOM '03, Vol. 3, San Francisco, CA, 2003, pp. 1987–1997.

[6] L. Buttyán, J.-P. Hubaux, Stimulating cooperation in self-organizing mobile ad hoc networks, ACM/Kluwer Mobile Networks and Applications 8 (5) (2003) 579–592.

[7] J. Crowcroft, R. Gibbens, F. Kelly, S. Östring, Modelling incentives for collaboration in mobile ad hoc networks, in: Proc. WiOpt '03, France, 2003.

[8] L. Anderegg, S. Eidenbenz, Ad hoc-VCG: A truthful and cost-efficient routing protocol for mobile ad hoc networks with selfish agents, in: Proc. ACM Ninth Annual International Conference on Mobile Computing and Networking (MobiCom '03), San Diego, CA, 2003, pp. 245–259.

[9] S. Marti, T. J. Giuli, K. Lai, M. Baker, Mitigating routing misbehavior in mobile ad hoc networks, in: Proc. Sixth Annual International Conference on Mobile Computing and Networking (MobiCom '00), Boston, MA, 2000, pp. 255–265.

[10] P. Michiardi, R. Molva, CORE: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks, in: Proc. Communications and Multimedia Security Conference (CMS '02), Portoroz, Slovenia, 2002.

[11] S. Buchegger, J.-Y. Le Boudec, Performance analysis of the CONFIDANT protocol (cooperation of nodes: Fairness in dynamic ad-hoc networks), in: Proc. International Symposium on Mobile Ad Hoc Networking & Computing (MobiHoc '02), Lausanne, Switzerland, 2002, pp. 226–236.

[12] S. Bansal, M. Baker, Observation-based cooperation enforcement in ad hoc networks, Tech. rep., Stanford University, Stanford, CA (Jul. 2003).

[13] Q. He, D. Wu, P. Khosla, SORI: A secure and objective reputation-based incentive scheme for ad-hoc networks, in: Proc. IEEE Wireless Communications and Networking Conference (WCNC '04), Vol. 2, Atlanta, GA, 2004, pp. 825–830.

[14] R. Mahajan, M. Rodrig, D. Wetherall, J. Zahorjan, Sustaining cooperation in multi-hop wireless networks, in: Proc. Second Symposium on Networked Systems Design and Implementation (NSDI '05), Boston, MA, 2005.

[15] P. Michiardi, R. Molva, Analysis of coalition formation and cooperation strategies in mobile ad hoc networks, Ad Hoc Networks 3 (2) (2005) 193–219.

[16] M. T. Refaei, V. Srivastava, L. DaSilva, M. Eltoweissy, A reputation-based mechanism for isolating selfish nodes in ad hoc networks, in: Proc. IEEE Second Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous '05), San Diego, CA, 2005, pp. 3–11.

[17] T. Anantvalee, J. Wu, Reputation-based system for encouraging the cooperation of nodes in mobile ad hoc networks, in: Proc. IEEE International Conference on Communications (ICC), Glasgow, Scotland, 2007, pp. 3383–3388.

[18] D. Fudenberg, J. Tirole, Game Theory, The MIT Press, Cambridge, MA, 1991.

[19] R. Axelrod, The emergence of cooperation among egoists, The American Political Science Review 75 (2) (1981) 306–318.

[20] F. Milan, J. J. Jaramillo, R. Srikant, Achieving cooperation in multihop wireless networks of selfish nodes, in: Workshop on Game Theory for Networks (GameNets 2006), Pisa, Italy, 2006.

[21] J. Wu, R. Axelrod, How to cope with noise in the iterated prisoner's dilemma, The Journal of Conflict Resolution 39 (1) (1995) 183–189.

[22] R. Sugden, The Economics of Rights, Cooperation and Welfare, Blackwell Publishing, 1986.

[23] R. Boyd, Mistakes allow evolutionary stability in the repeated prisoner's dilemma game, Journal of Theoretical Biology 136 (1) (1989) 47–56.

[24] M. Abadi, M. Burrows, M. Manasse, T. Wobber, Moderately hard, memory-bound functions, ACM Transactions on Internet Technology 5 (2) (2005) 299–327.

[25] C. Dwork, A. Goldberg, M. Naor, On memory-bound functions for fighting spam, in: Proc. 23rd Annual International Cryptology Conference (CRYPTO '03), Santa Barbara, CA, 2003.

[26] W. Diffie, M. E. Hellman, New directions in cryptography, IEEE Transactions on Information Theory IT-22 (6) (1976) 644–654.

[27] R. Anderson, M. Kuhn, Tamper resistance - a cautionary note, in: Proc. Second USENIX Workshop on Electronic Commerce, Oakland, CA, 1996, pp. 1–11.

[28] S. Sundaram, C. N. Hadjicostis, Distributed function calculation via linear iterations in the presence of malicious agents - Part I: Attacking the

network, in: Proc. 27th American Control Conference (ACC), Seattle, WA, 2008, pp. 1350–1355.

[29] S. Sundaram, C. N. Hadjicostis, Distributed function calculation via linear iterations in the presence of malicious agents - Part II: Overcoming malicious behavior, in: Proc. 27th American Control Conference (ACC), Seattle, WA, 2008, pp. 1356–1361.